UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,424	04/10/2006	Yang Peng	CN 030035	3752

24737 7590 09/28/2010
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
09/28/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/575,424	PENG ET AL.	
	Examiner	Art Unit	
	JEFFREY D. POPHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 17-32 are pending.

Response to Arguments

1. Applicant's arguments filed 7/14/2010 have been fully considered but they are not persuasive.

Applicant argues that "In prior systems, while the server might be authentic, external media content residing on it might be compromised (e.g., see, present application, paragraphs [0007]-[0009]). Therefore, in accordance with the present system, the external media content of the server is authenticated independent of any authentication of the server that may or may not be performed." It is noted that nothing in the claims states that the content is signed or provided with any authenticity data prior to storing the content on the server. It is further noted that the claims are not directed to servers, but rather, to "one or more computing devices distributed on a network" on which the external media content is provided. This could be a server, a client, a PC, a phone, or any "computing device" which provides the external media content in any form (e.g. sending, storing, rendering for a user, etc.). Therefore, stating that "authenticity of the external media content is verified independent of the authenticity of the one or more computing devices on which the external media content is provided" merely means that authentication of the external media content is performed independently of some device that "provides" the external media content. As an example, since the video reproduction apparatus of Kambayashi provides the

external media content by storing and rendering such external media content, this video reproduction apparatus meets the "one or more computing devices distributed on a network" portion of claim 20. Clearly, certifying/authenticating the downloaded ENAV/V-click data within Kambayashi within the video reproduction apparatus is independent of authenticating the video reproduction apparatus. Other examples of what could meet the one or more computing devices of the claims would be other content distribution servers not providing the ENAV/V-click data to the client, proxies, routers, gateways, and the like, all of which provide the content and are distributed on a network. It will be further shown below that, even when server 7 of Kambayashi is interpreted as the one or more computing devices of claim 20, Kambayashi still meets the claimed limitations.

Applicant argues that "authentication of a server is not the same as authentication of external media content downloaded from the server." Applicant goes on to argue that "the claims of the present invention set out authenticating external media content downloaded from the server and are unrelated to authenticating the server." However, as described above, the claims never recite a server. Furthermore, the claims never recite downloading of the external media content from a server, as there is no server discussed in the claims. Further still, the claims do not recite downloading of the external media content from the one or more computing devices. Therefore, the entity from which Kambayashi downloads the ENAV/V-click data need not be the "one or more

computing devices" as claimed. As just described, any computing device that provides the external media content in any way meets this limitation.

Applicant argues that "It is undisputed that Kumbayashi (*sic*) does not teach, disclose or suggest a "public key provided on an optical disk on which the media content is stored" or "a control system to verify the authenticity of the downloaded external media content using the public key read-out from the optical disk before the stored media content is played in coordination with the associated downloaded external media content" as for example recited in claim 20. (See Office Action, page 6, fourth paragraph). The Office Action references Uranaka at cols. 6, 7, 8, and 12 to provide that which is admitted missing from Kumbayashi, however, it is respectfully submitted that reliance on these portions of Uranaka or any portions for that matter is misplaced." However, the only thing portion of claim 20 that is not explicitly disclosed within Kambayashi is "that the public key is read from the optical disk" (See, Office Action, page 6, fourth paragraph). Kambayashi teaches every other aspect of claim 20. With respect to Applicant's arguments regarding Kambayashi, Applicant argues that "as stated in Kumbayashi, paragraphs [0216] and [0239], Kumbayashi uses "a public key P_k corresponding to the secret key S_k of the server" not corresponding to external media content." However, if content is encrypted with a secret key S_k and authenticated with a public key P_k, that secret key and public key are clearly "corresponding to the external media content." Further, the claims do not provide any correspondence of the public key to the external media content. The private key and public key are not generated specifically for this piece of content, nor are

they only used for this particular piece of content. All that is required by the claim, with respect to this public key, is that the authenticity of the downloaded external media content is verified using a public key read out from the optical disk. Kambayashi teaches verifying the authenticity of downloaded external media content using a public key, and Uranaka teaches that the public key is read out from an optical disk.

The Kambayashi teachings are found in authenticating the ENAV (e.g. V-click) data in the previously cited portions, as set forth in the previous office action, as well as figures 21-22 and the corresponding description thereof. In figure 21, step S406, it is determined whether the server is certified (authentic). In step S409, it is determined whether the data is certified (authentic). Step S409 (certification of the ENAV/V-click data) is further discussed with respect to figure 22. Figure 22 clearly shows decoding the data using the public key P_k, decoding the data using content ID (CID), and determining whether the data is certified (authentic).

Clearly, as Kambayashi explicitly separates certification of the server from certification of the data, the authenticity/certification of the downloadable content is independent of authenticity/certification of the server, as the server was authenticated prior to authentication of the data. Kambayashi further goes on to state that "the certification of the server 7 that provides ENAV contents 103 or that of V-click data, or both may be omitted." This further shows the distinction, in that the server need not even be authenticated/certified within Kambayashi, but rather, such certification of the server may be omitted, leaving only

certification of the ENAV contents. Therefore, Kambayashi clearly and explicitly teaches that authentication of the content is independent of authentication of the server, as each is performed in a completely distinct step. It is insignificant that the secret key S_K is "of the server" in Kambayashi due to this explicit segregation of certifying/authenticating the server and certifying/authenticating the ENAV/V-click data.

With respect to Uranaka, Applicant argues that "Uranaka describes a **server** public key, e.g., distribution descriptor 23 recorded in the burst cutting area of the DVD, (see, Uranaka, col. 12, lines 12-15) for verifying authenticity of a specific server." As Kambayashi explicitly teaches that authentication of the ENAV/V-click data is performed using the public key corresponding to a secret key of the server and is performed independently of authentication of the server itself, this is a moot point, as Uranaka teaches that the public key of the combination is stored on an optical disk. This should be clear from the fact that Kambayashi teaches the public key being used to certify/authenticate the ENAV/V-click data as corresponding to the secret key of the server. Therefore, Uranaka's teachings of providing a public key corresponding to a server on the optical disk is in line with that of Kambayashi.

Applicant goes on to argue that "Kumbayashi, Uranaka, Ryan, Collins, and Tsumagari do not teach, disclose, or suggest a private key added to the external media content that is being authenticated" without providing any reason as to why Applicant believes this to be the case. Clearly, Kambayashi teaches such in paragraph 240, for example, stating that "the server 7 further encodes E(CID)[H]

using S_k, which is the secret/private key corresponding to the public key used in certification/authentication of the data.

Claim Objections

2. Claims 24 and 31 are objected to because of the following informalities: Claim 24 states that "the control system verifies the authenticity of the downloaded external media content by performing asymmetric cryptography using the public key stored on the optical disk and a corresponding private key encrypted the downloaded external media content." However, when one looks to the written description, it appears as though this public key and private key are the 2 keys of a key pair (Page 7, for example, showing that the private key of the downloaded content and the public key that is stored on the disk are part of the same key pair). One will further note that the control system only has access to the public key retrieved from the optical disk, and never sees the private key. Furthermore, if the control system were to perform asymmetric cryptography operations with both the public key as well as the private key from the same key pair, as claimed, the operations would cancel each other out, since one key would encrypt and the other would decrypt. For purposes of prior art rejection, this has been construed as "the control system verifies the authenticity of the downloaded external media content by performing asymmetric cryptography using the public key stored on the optical disk corresponding to a private key used to encrypt the downloaded external media content." Claim 31 has the same issue and has been interpreted in the same fashion.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 17, 18, 20, 22, 24, 25, 27-29, 31, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kambayashi (U.S. Patent Application Publication 2004/0001697) in view of Uranaka (U.S. Patent 6,470,085)

Regarding Claim 20,

Kambayashi discloses an optical disk player comprising:

An optical disk driver unit to read out stored media content provided on an optical disk on which the media content is stored (Figures 1 and 18; and Paragraph 47);

A network interface to download one or more external media content, each external media content having an added private key and is associated with at least one stored media content, the one or more external media content provided on one or more computing devices distributed on a network (Figures 1, 18, and 21-22; and Paragraphs 205, 209, 212, 216, 240, and 246); and

A control system to verify the authenticity of the downloaded external media content using a public key that was obtained before the stored media content is played in coordination with the associated downloaded external media content (Figures 21-22; and Paragraphs 216-221 and 231-244);

Wherein the authenticity of the external media content is verified unaware of the authenticity of the one or more computing devices on which the external media content is provided (Figures 21-22; and Paragraphs 216-221 and 231-244);

But does not appear to explicitly disclose that the public key is read from the optical disk.

Uranaka, however, discloses that the public key is read from the optical disk (Column 6, lines 42-54; Column 7, lines 9-33; Column 8, lines 23-41; and Column 12, lines 12-15). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content usage control system of Uranaka into the enhanced content reproduction system of Kambayashi in order to ensure that a user has been given an appropriate public key by sending it on the disk along with the content, and/or to allow the system to restrict content access to those devices that a server deems authorized to do so.

Regarding Claim 17,

Claim 17 is a system claim that is broader than player claim 20 and is rejected for the same reasons.

Regarding Claim 25,

Claim 25 is a method claim that is broader than player claim 20 and is rejected for the same reasons.

Regarding Claim 22,

Kambayashi as modified by Uranaka discloses the player of claim 20, in addition, Kambayashi discloses that the downloaded external media content is an application program (Paragraph 220, script in ENAV contents, for example).

Regarding Claim 29,

Claim 28 is a method claim that is broader than player claim 29 and is rejected for the same reasons.

Regarding Claim 24,

Kambayashi as modified by Uranaka discloses the player of claim 20, in addition, Kambayashi discloses that the control system verifies the authenticity of the downloaded external media content by performing asymmetric cryptography using the public key stored on the optical disk and corresponding to a private key used to encrypt the downloaded external media content (Figures 2—22; Paragraphs 216-221 and 231-244).

Regarding Claim 31,

Claim 31 is a method claim that is broader than player claim 24 and is rejected for the same reasons.

Regarding Claim 18,

Kambayashi as modified by Uranaka discloses the system of claim 17, in addition, Uranaka discloses that the public key is stored in a BCA zone of the optical disk (Figures 2 and 4; Column 5, lines 20-42; Column 5, line 58 to Column 6, line 5; and Column 8, lines 34-41).

Regarding Claim 27,

Kambayashi as modified by Uranaka discloses the method of claim 25, in addition, Kambayashi discloses that the coordination between the read out stored media content and the downloaded external media content will not be established if the downloaded external media content is not authenticated (Figures 21-22; and Paragraph 234).

Regarding Claim 28,

Kambayashi as modified by Uranaka discloses the method of claim 27, in addition, Kambayashi discloses that the coordination between the read out stored media content and downloaded external media content will be established if the downloaded external media content is authenticated (Figure 21; and Paragraph 234).

Regarding Claim 32,

Kambayashi as modified by Uranaka discloses the method of claim 25, in addition, Kambayashi discloses that the optical disk comprises digital information stored thereon, the stored digital information comprising network address information that is used to download the external media content (Paragraph 209); and Uranaka discloses that the optical disk comprises a public key that is used to verify the authenticity of the downloaded external media content before playing the stored media content in coordination with the external media content (Figures 2 and 4; Column 5, lines 20-42; Column 5, line 58 to Column 6, line 5; and Column 15, lines 57-67).

4. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kambayashi in view of Uranaka, further in view of Ryan (U.S. Patent 5,754,648).

Kambayashi as modified by Uranaka does not explicitly disclose that the public key is stored in a media content zone of the optical disk.

Ryan, however, discloses that the public key is stored in a media content zone of the optical disk (Column 3, lines 47-67; and Column 8, lines 31-37). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the media security and tracking system of Ryan into the enhanced content reproduction system of Kambayashi as modified by Uranaka in order to allow the system to provide additional authentication and authorization steps such that a device can ensure that both the disk and device are authentic and

authorized for use with each other by using data stored on the optical disk itself and data stored on a magnetic track attached to the disk, thus decreasing the chance of unauthorized use thereof, and/or to provide the ability to track use of the media.

5. Claims 21 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kambayashi in view of Uranaka, further in view of Collins (U.S. Patent Application Publication 2002/0073316).

Regarding Claim 21,

Kambayashi as modified by Uranaka does not explicitly disclose that the control system detects whether the downloaded external media content is integral before verification, wherein the verification will not be executed if the downloaded external media content is detected to not be integral.

Collins, however, discloses that the control system detects whether the downloaded external media content is integral before verification, wherein the verification will not be executed if the downloaded external media content is detected to not be integral (Paragraphs 73-77; detecting whether the downloaded content is "integral" may comprise either, or both, verification of the program packet format and/or verification of the checksum, each of which must succeed before signature verification is performed). It would have been obvious to one of ordinary skill in the art at the time of

applicant's invention to incorporate the content authentication and access control system of Collins into the enhanced content reproduction system of Kambayashi as modified by Uranaka in order to allow the system to detect when errors in the data have occurred, such that data with errors will not be allowed to be processed and only correct data will be processed, and/or to ensure that the data is proper and authentic before allowing access to proceed, thereby increasing security of the system by ensuring both integrity and authenticity of the content.

Regarding Claim 26,

Claim 26 is a method claim that is broader than player claim 21 and is rejected for the same reasons.

6. Claims 23 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kambayashi in view of Uranaka, further in view of Tsumagari (U.S. Patent Application Publication 2004/0126095).

Regarding Claim 23,

Kambayashi as modified by Uranaka does not explicitly disclose that the application program is a JAVA language application program.

Tsumagari, however, discloses that the application program is a JAVA language application program (Figure 10; and Paragraphs 143 and 167). It would have been obvious to one of

ordinary skill in the art at the time of applicant's invention to incorporate the script execution system of Tsumagari into the enhanced content reproduction system of Kambayashi as modified by Uranaka in order to allow the system to work with various kinds of well-known languages, thereby allowing additional flexibility in the creation of ENAV contents as well as allowing a broader range of devices to take advantage of the ENAV contents.

Regarding Claim 30,

Claim 30 is a method claim that is broader than player claim 23 and is rejected for the same reasons.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437